View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Electronic Archive of Kyiv Polytechnic Institute

УДК 004.056.53+004.057.4

РЕАЛИЗАЦИЯ ПРОТОКОЛОВ КОЛЛЕКТИВНОЙ ПОДПИСИ НА ОСНОВЕ СТАНДАРТОВ ГОСТ 34.310–95 И ДСТУ 4145-2002

Лидия Гортинская, Николай Молдовян, Галина Козина*

*Научный филиал ФГУП НИИ «Вектор» - Специализированный центр программных систем «СПЕКТР», *Запорожский национальный технический университет*

Аннотация: **Рассмотрены стандарты электронной цифровой подписи, действующие в России и в Украине. Предложены протоколы коллективной электронной цифровой подписи на основе этих стандартов.**

Summary: **The electronic digital signature standards, operating in Russia and on Ukraine, are considered. Protocols of collective electronic digital signature on the basis of these standards are offered.**

Ключевые слова: **Электронная цифровая подпись, коллективная подпись, стандарты электронной цифровой подписи.**

I Введение

В технологиях электронного документооборота широко используются алгоритмы электронной цифровой подписи (ЭЦП), на основе которых в сочетании с нормативно-правовыми механизмами обеспечивается придание юридической силы электронным документам [1, 2]. При разработке коллективных проектов важной проблемой является реализация протоколов [3], обеспечивающих реализацию коллективной (или кратной) электронной цифровой подписи (КЭЦП).

Подходы к решению этой задачи на основе генерации совокупности ЭЦП, принадлежащей отдельным пользователям, имеют следующие недостатки. Требуется использовать дополнительные процедуры проверки целостности КЭЦП, которые позволяют проверить ее полноту, т. е. обнаружить попытки формирования КЭЦП, принадлежащей измененному числу пользователей. Другим недостатком является увеличение размера КЭЦП пропорционально числу подписавших участников. Особенно важен вопрос минимизации размера КЭЦП при необходимости ее записи в виде штрих-кода на бумажных носителях, например, в методах защиты от подделки документов с помощью электронной цифровой подписи [4]. Для устранения указанных недостатков недавно был предложен новый способ [5] формирования и проверки подлинности КЭЦП с использованием общего (коллективного) открытого ключа, формируемого на основе индивидуальных открытых ключей систем ЭЦП, применяемых на практике. Возможность использования (доступность через Internet) стандартных справочников открытых ключей и/или типовых сертификатов открытых ключей благоприятствует практическому применению нового подхода генерации КЭЦП. В данном аспекте представляет интерес изучение вопроса о возможности реализации новых протоколов КЭЦП с использованием процедур проверки ЭЦП, специфицируемых стандартами подписи.

В настоящей работе исследуется вопрос о реализации протоколов КЭЦП на основе стандартов ЭЦП ГОСТ 34.310–95 [2, 6] и ДСТУ 4145-2002 [7, 8].

II Реализация протокола коллективной подписи на основе стандарта электронной цифровой подписи ГОСТ 34.310–95

Общесистемные параметры

Стандарт ГОСТ 34.310–95 регламентирует использование простого числа p, такого что $510 \le |p| \le 512$ бит либо $1022 \le |p| \le 1024$ бит, где $|p|$ – разрядность p в двоичном представлении, причем число $p-1$ содержит большой простой делитель q: $2^{255} \le q \le 2^{256}$ либо $2^{511} \le q \le 2^{512}$, соответственно. Специфицируемые алгоритмы генерации и проверки электронной цифровой подписи используют число α – генератор подгруппы порядка q (т. е. q является наименьшим числом, для которого выполняется условие $\alpha^q \bmod p = 1$).

Процедуры формирования и проверки подписи в стандарте ГОСТ 34.310–95

Секретный ключ пользователя представляет собой случайно генерируемое число d, $1 < d < q$.

Соответствующий ему открытый ключ y вычисляется по формуле $y = \alpha^d \bmod p$.

Генерация электронной цифровой подписи осуществляется следующим образом.

1. Выбирается случайное число k, $1 < k < q$.
2. Вычисляется значение

$$R = \left(\alpha^k \bmod p\right) \bmod q, \tag{1}$$

являющееся первой частью подписи.

3. По стандарту ГОСТ 34.311–95 [9] вычисляется хэш-образ H от подписываемого пользователем электронного документа.

4. Вычисляется вторая часть подписи:

$$S = \left(kH + dR\right) \bmod q. \tag{2}$$

Если S = 0, то процедура генерации подписи повторяется.

Процедура проверки подлинности электронной цифровой подписи (R, S) выполняется следующим образом:

1. Проверяется выполнение условий $R < q$ и $S < q$. Если они не выполняются, то подпись недействительна.

2. По стандарту ГОСТ 34.311–95 вычисляется хэш-образ H от принятого электронного документа.

3. С использованием открытого ключа y пользователя, подписавшего документ, вычисляется значение

$$R' = \left(\alpha^{S/H} y^{-R/H} \bmod p\right) \bmod q. \tag{3}$$

3. Сравниваются значения R' и R: если $R' = R$, подпись признается действительной, в противном случае отвергается.

Протокол коллективной подписи на основе ГОСТ 34.310–95

В протоколе КЭЦП используются те же общесистемные параметры p, q и α.

Протокол КЭЦП реализуется следующим образом.

Каждый i-ый ($i = 1, 2, \ldots, t$) пользователь формирует открытый ключ вида $y_i = \alpha^{d_i} \bmod p$, где d_i – личный (секретный) ключ i-ого пользователя, $1 < d_i < q$.

Коллективным открытым ключом y является произведение

$$y = \prod_{i=1}^{t} y_i \bmod p. \tag{4}$$

Для формирования коллективной подписи используется следующий алгоритм.

Каждый подписывающий выбирает разовый случайный секретный ключ – число k_i, $(1 < k_i < q)$, а затем вычисляет $R_i = (\alpha^{k_i} \bmod p) \bmod q$ и предоставляет это значение для коллективного использования.

Далее вычисляется произведение

$$R = \prod_{i=1}^{t} R_i \bmod p. \tag{5}$$

Затем каждый пользователь по своему значению R_i и величине H (хэш-образу общего электронного документа, полученного с использованием функции хэширования ГОСТ 34.311–95) вычисляет свою долю подписи $S_i = (k_i H + d_i R) \bmod q$.

Коллективной подписью является пара чисел (R, S), где S вычисляется по формуле

$$S = \sum_{i=1}^{t} S_i \bmod q. \tag{6}$$

Проверка коллективной подписи (R, S) осуществляется с помощью коллективного открытого ключа y пользователей, подписавших документ, по проверочной формуле

$$R' = \left(\alpha^{S/H} y^{-R/H} \bmod p\right) \bmod q, \tag{7}$$

где H – хэш-образ принятого общего электронного документа, полученного с использованием функции хэширования ГОСТ 34.311–95.

Если $R' = R$, то КЭЦП совокупности пользователей $1, 2, \ldots, t$ является подлинной, так как она могла быть сформирована только при участии каждого пользователя из этой группы, и для ее формирования требуется использование секретного ключа каждого из них. Отметим, что аутентификация значений R_i осуществляется автоматически при проверке подлинности КЭЦП. Если нарушитель попытается осуществить подмену какого-нибудь из этих значений, то факт вмешательства в протокол будет сразу же выявлен при проверке подлинности КЭЦП, т. е. будет получено $R' \neq R$. Видно, что размер КЭЦП не зависит от числа пользователей t.

Покажем корректность предложенного алгоритма КЭЦП. Подставив подпись (*R*, *S*), где параметры *R* и *S* определяются формулами (5) и (6) соответственно, в проверочное уравнение (7), убеждаемся, что выполняется равенство *R′*=*R*:

$$R' = \left(\alpha^{S/H} y^{-R/H} \bmod p\right) \bmod q = \left(\alpha^{\sum_{i=1}^{t} S_i/H} \left(\prod_{i=1}^{t} y_i \right)^{-R/H} \bmod p \right) \bmod q =$$

$$= \left(\prod_{i=1}^{t} \alpha^{S_i/H} \cdot \prod_{i=1}^{t} y_i^{-R/H} \bmod p \right) \bmod q = \left(\prod_{i=1}^{t} \alpha^{S_i/H} \cdot y_i^{-R/H} \bmod p \right) \bmod q =$$

$$= \left(\prod_{i=1}^{t} \alpha^{k_i + d_i R/H} \cdot \left(\alpha^{d_i}\right)^{-R/H} \bmod p \right) \bmod q = \left(\prod_{i=1}^{t} \alpha^{k_i} \bmod p \right) \bmod q =$$

$$= \left(\left(\prod_{i=1}^{t} \alpha^{k_i} \bmod p \right) \bmod q \right) \bmod q = \left(\prod_{i=1}^{t} R_i \right) \bmod q = R.$$

Таким образом, корректность предложенного алгоритма КЭЦП на основе стандарта ГОСТ 34.310–95 доказана.

III Реализация протокола коллективной подписи на основе стандарта электронной цифровой подписи ДСТУ 4145-2002

Общесистемные параметры

Общесистемные параметры в данном стандарте определены таким образом:

$GF(2^m)$ – основное поле Галуа как *m*-кратное расширение простого поля $GF(2)$;

m – простое число в интервале [163, 509];

E: $y^2 + xy = x^3 + ax^2 + b$ – несуперсингулярная эллиптическая кривая над полем $GF(2^m)$ с порядком $N_E = cn$ и коэффициентами $a = 0$ или $a = 1$ и $b \neq 0$;

P – точка эллиптической кривой E простого порядка *n*, $n > 2^{160}$;

H(•) — некоторая хэш-функция. Допускается как использование стандарта [9], так и других стандартов функций хэширования.

Вычисления в поле производятся в полиномиальном или оптимальном нормальном базисах.

Процедуры формирования и проверки подписи в стандарте ДСТУ 4145-2002

Секретный ключ пользователя представляет собой случайно генерируемое число *d*, $1 < d < n$. Соответствующий ему открытый ключ *Q* вычисляется как точка эллиптической кривой по формуле $Q = -dP$.

Генерация ЭЦП осуществляется следующим образом.

1. Выбирается случайное число *k*, $1 < k < n$.

2. Вычисляется точка эллиптической кривой

$$R = kP = (x_R, y_R). \qquad (8)$$

Если $x_R = 0$, то возврат в п. 1.

3. Вычисляется значение хэш-образа *H* от подписываемого пользователем электронного документа. Значение хэш-образа *H* интерпретируется как элемент *h* основного поля $GF(2^m)$.

4. Вычисляется элемент поля $y = hx_R$. При $y = 0$ возврат к п. 1.

5. Элемент поля *y* преобразуется в целое десятичное число *r*: в битовом представлении элемента *y* поля $GF(2^m)$ используются младшие $|n| - 1$ разрядов, которые формируют десятичное число *r*. При $r = 0$ выполняется возврат в п. 1.

Число *r* является первой частью подписи.

6. Вычисляется вторая часть подписи:

$$s = (k + dr) \bmod n. \qquad (9)$$

Если $s = 0$, то процедура генерации подписи повторяется.

Процедура проверки подлинности электронной цифровой подписи (*R*, *S*) выполняется следующим

образом.

1. Поверяется выполнение условий $0 < r < n$ и $0 < s < n$. Если они не выполняются, то подпись недействительна.

2. С помощью открытого ключа Q пользователя, подписавшего документ, вычисляется точка R' эллиптической кривой

$$R' = sP + rQ = \left(x_{R'}, y_{R'}\right). \tag{10}$$

3. Вычисляется значение хэш-образа H от принятого электронного документа. Значение хэш-образа H интерпретируется как элемент h основного поля $GF(2^m)$.

4. Вычисляется элемент поля $y = hx_R'$. Элемент поля y преобразуется в целое десятичное число r' : в битовом представлении элемента y поля $GF(2^m)$ используются младшие $|n|-1$ разрядов, которые формируют десятичное число r'.

5. Сравниваются значения r' и r: если $r' = r$, подпись признается действительной, в противном случае отвергается.

Протокол коллективной подписи на основе ДСТУ 4145-2002

В протоколе КЭЦП используются те же общесистемные параметры $GF(2^m)$, E, P и n.

Протокол КЭЦП реализуется следующим образом.

Каждый i-ый ($i = 1, 2, \ldots, t$) пользователь формирует открытый ключ вида $Q_i = -d_iP$, где d_i – личный (секретный) ключ, $1 < d_i < q$.

Коллективным открытым ключом является сумма точек эллиптической кривой

$$Q = \sum_{i=1}^{t} Q_i \,. \tag{11}$$

Для формирования коллективной подписи используется следующий алгоритм.

Каждый подписывающий выбирает разовый случайный секретный ключ – число k_i, $(1 < k_i < n)$, а затем вычисляет координаты точки $R_i = k_i\, P$ и предоставляет их для коллективного использования.

Далее вычисляется сумма всех точек R_i:

$$R = \sum_{i=1}^{t} R_i = (x_R, y_R)\,, \tag{12}$$

по которой вычисляется значение r – первой части коллективной подписи.

Вычисляется значение хэш-образа H от подписываемого общего электронного документа. Значение хэш-образа H интерпретируется как элемент h основного поля $GF(2^m)$. Вычисляется элемент поля $y = hx_R$.

Элемент поля y преобразуется в целое десятичное число r: в битовом представлении элемента y поля $GF(2^m)$ используются младшие $|n|-1$ разрядов, которые формируют десятичное число r. При $r = 0$ выполняется возврат в п. 1.

Затем каждый пользователь по своему секретному ключу d_i и значению k_i вычисляет свою долю подписи $s_i = (k_i + d_i\, r) \bmod n$.

Коллективной подписью является пара чисел (r, s), где s вычисляется по формуле

$$s = \sum_{i=1}^{t} s_i \bmod n\,. \tag{13}$$

Проверка коллективной подписи (r, s) осуществляется следующим образом.

С помощью общего открытого ключа Q пользователей, подписавших документ, вычисляется точка R' эллиптической кривой

$$R' = sP + rQ = \left(x_{R'}, y_{R'}\right). \tag{14}$$

Далее вычисляется значение хэш-образа H от принятого электронного документа. Значение хэш-образа H интерпретируется как элемент h основного поля $GF(2^m)$. Вычисляется элемент поля $y = hx_R'$. Элемент поля y преобразуется в целое десятичное число r' : в битовом представлении элемента y поля $GF(2^m)$ используются младшие $|n| - 1$ разрядов, которые формируют десятичное число r'.

Сравниваются значения r' и r.

Если $r' = r$, то КЭЦП совокупности пользователей $1, 2, \ldots, t$ является подлинной, так как она могла быть сформирована только при участии каждого пользователя из этой группы и для ее формирования требуется использование секретных ключей каждого из них. Если нарушитель попытается осуществить подмену какого-нибудь из этих значений, то факт вмешательства в протокол будет сразу же выявлен при проверке подлинности КЭЦП, т. е. будет получено $r' \neq r$. Видно, что размер КЭЦП не зависит от числа

пользователей t.

Покажем корректность предложенного алгоритма КЭЦП. Подставив подпись (r, s) в проверочное уравнение (14) убеждаемся, что выполняется равенство $R'=R$:

$$R' = sP + rQ = \left(\sum_{i=1}^{t} s_i \right) P + r \sum_{i=1}^{t} Q_i = \sum_{i=1}^{t} \left(s_i P + r Q_i \right) =$$

$$= \sum_{i=1}^{t} \left(\left(k_i + d_i r \right) P + r \left(-d_i P \right) \right) = \sum_{i=1}^{t} \left(k_i P \right) = \sum_{i=1}^{t} R_i = R .$$

Поскольку $R' = R$, то также выполняется и $r' = r$.

Таким образом, корректность предложенного алгоритма КЭЦП на основе стандарта ДСТУ 4145-2002 доказана.

IV Заключение

Применение понятия коллективного открытого ключа, вычисляемого как свертка подмножества индивидуальных открытых ключей, позволяет построить протоколы КЭЦП, перспективные для практического применения в технологиях электронного документооборота, благодаря обеспечению одновременности формирования подписи и ее целостности. Для произвольной совокупности пользователей может быть легко выработан соответствующий им коллективный ключ, на основе которого можно проверить их коллективную подпись. Достоинством предложенных протоколов является возможность их практической реализации на основе стандартной инфраструктуры открытых ключей и стандартов электронной цифровой подписи ГОСТ 34.310-95 и ДСТУ 4145-2002. Учитывая аналогию стандартов ГОСТ 34.310-95 и ГОСТ Р 34.10-2001, легко показать, что рассматриваемый подход формирования КЭЦП может быть реализован также и на основе последнего стандарта.

Использование КЭЦП представляет удачное решение известной проблемы одновременного подписания контракта [10]. Представляет интерес использование КЭЦП и для построения протоколов «множественной подписи» [10], что составляет самостоятельную задачу дальнейшего развития протоколов на основе понятия коллективного открытого ключа.

*Литература: **1**. Венбо Мао. Современная криптография. Теория и практика. - М., СПб., Киев: Издательский дом «Вильямс», 2005. - 763 с. **2.** Молдовян Н. А. Введение в криптосистемы с открытым ключом. – Санкт-Петербург: БХВ-Петербург, 2005. – 286 с. **3.** Min-Shiang Hawng, Cheng-Chi Le: Research issues and challenges for multiple digital signature, Int. J. of Network Security, 2005. Vol. 1. No 1, pp. 1-7. **4.** Карякин Ю. Д. Технология «AXIS-2000» защиты материальных объектов от подделки // «Управление защитой информации». – М.: 1997. – Т.1. – № 2. – С. 90-97. **5.** Молдовян Н. А., Молдовян П. А. Новые протоколы слепой подписи // «Безопасность информационных технологий». – М.: 2007. – № 3. – С. 17-21. **6.** Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. Межгосударственный стандарт ГОСТ 34.310-95. – 16 с. **7.** Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірка. Держстандарт України ДСТУ 4145-2002. – 94 с. **8.** Беспалов А. В., Телиженко А. Б. Криптосистемы на эллиптических кривых: Учеб.пособие. – К.: ІВЦ "Видавництво «Політехніка»", 2004. – 224 с. **9.** Информационная технология. Криптографическая защита информации. Функция хэширования. Межгосударственный стандарт ГОСТ 310. - 12 с. **10.** B. Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code (Second Edition) – New York.: John Wiley & Sons. – 1996. – 758 p.*

УДК 681.3.06

ТЕСТИРОВАНИЕ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ИСПОЛЬЗОВАНИЕМ КОНТЕКСТНОГО МОДЕЛИРОВАНИЯ

Виталий Шарапов

Физико-технический институт Национального технического университета Украины «КПИ»